Národní úřad
pro kybernetickou
a informační bezpečnost

Zabezpečení e-mailové komunikace s nZKB

TLP:CLEAR

TLP:CLEAR

Jakub Onderka

Bezpečnostní analytik, GovCERT.CZ, NÚKIB

E-mail: jakub.onderka@nukib.gov.cz
PGP: 2EEF A5E6 CAB0 A87F 4531 1FC3 B158 F39D C523 01CD
LinkedIn: https://www.linkedin.com/in/jakubonderka/

TLP:CLEAR

Jaký je současný stav zabezpečení e-mailů?

TLP:CLEAR

Zabezpečení e-mailové komunikace

10 %

TLP:CLEAR

Zabezpečení e-mailové komunikace

80 %

TLP:CLEAR

Zabezpečení e-mailové komunikace

10 %

TLP:CLEAR

Oportunistické šifrování STARTTLS

- Vzniklo v roce 1999, do té doby byl SMTP provoz kompletně nešifrovaný
- Zpětně kompatibilní metoda navazování zabezpečené komunikace

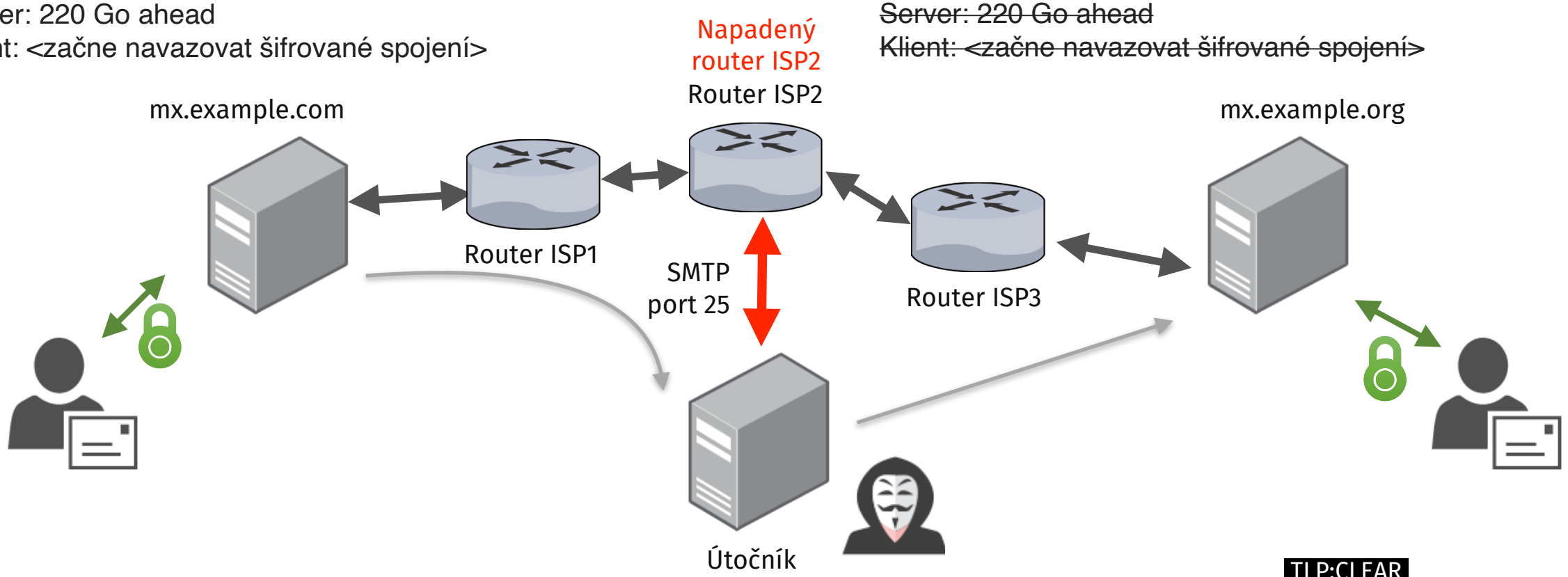
- Man in the middle (MITM, útok typu muže „uprostřed”) – útočník má přístup k prvku, skrz něj probíhá komunikace
- Pasivní MITM – pouze odposlouchávání komunikace (narušení důvěrnosti)
- Aktivní MITM – útočník má možnost komunikaci měnit (narušení integrity)

- **STARTTLS chrání pouze proti pasivnímu MITM!**

Zabezpečení e-mailové komunikace

Server: <čeká na spojení na portu 25>
Klient: <otevírá spojení>
Server: 220 mx.example.com ESMTP service ready
Klient: EHLO mx.examle.org
Server: 250-mx.example.com offers a warm hug of welcome
Server: 250 STARTTLS
Klient: STARTTLS
Server: 220 Go ahead
Klient: <začne navazovat šifrované spojení>

Server: <čeká na spojení na portu 25>
Klient: <otevírá spojení>
Server: 220 mx.example.com ESMTP service ready
Klient: EHLO mx.example.org
Server: 250-mx.example.com offers a warm hug of welcome
~~Server: 250 STARTTLS~~
~~Klient: STARTTLS~~
~~Server: 220 Go ahead~~
~~Klient: <začne navazovat šifrované spojení>~~



TLP:CLEAR

Co s tím?

Přece musí být řešení

- **Vynutit šifrování mezi servery**
- V současné době dvě konkurenční technologie (dají se použít oboje)
  - **DANE** (vyžaduje DNSSEC, standard používaný např. v Německu 2015)
  - **MTA-STS** (vyžaduje HTTPS, propaguje např. Google a Microsoft)
  - Ani jedna z nich nebyla (a stále není) široce podporována
  - **Aby správně fungovaly, musí je podporovat jak příjemce, tak odesilatel**

DANE

- DNS-Based Authentication of Named Entities
- Pro správnou funkci vyžaduje podporu DNSSEC
- RFC 7671, RFC 7672 pro SMTP
- Využívá speciální DNS záznam typu TLSA, který obsahuje otisk použitého certifikátu SMTP serveru

```
_25._tcp.mx.example.com. 262 IN TLSA
2 0 1 37834FA5EA40FBF7B61196955962E1CA0558872435E4206653D3F620DD8E988E
```

MTA-STS

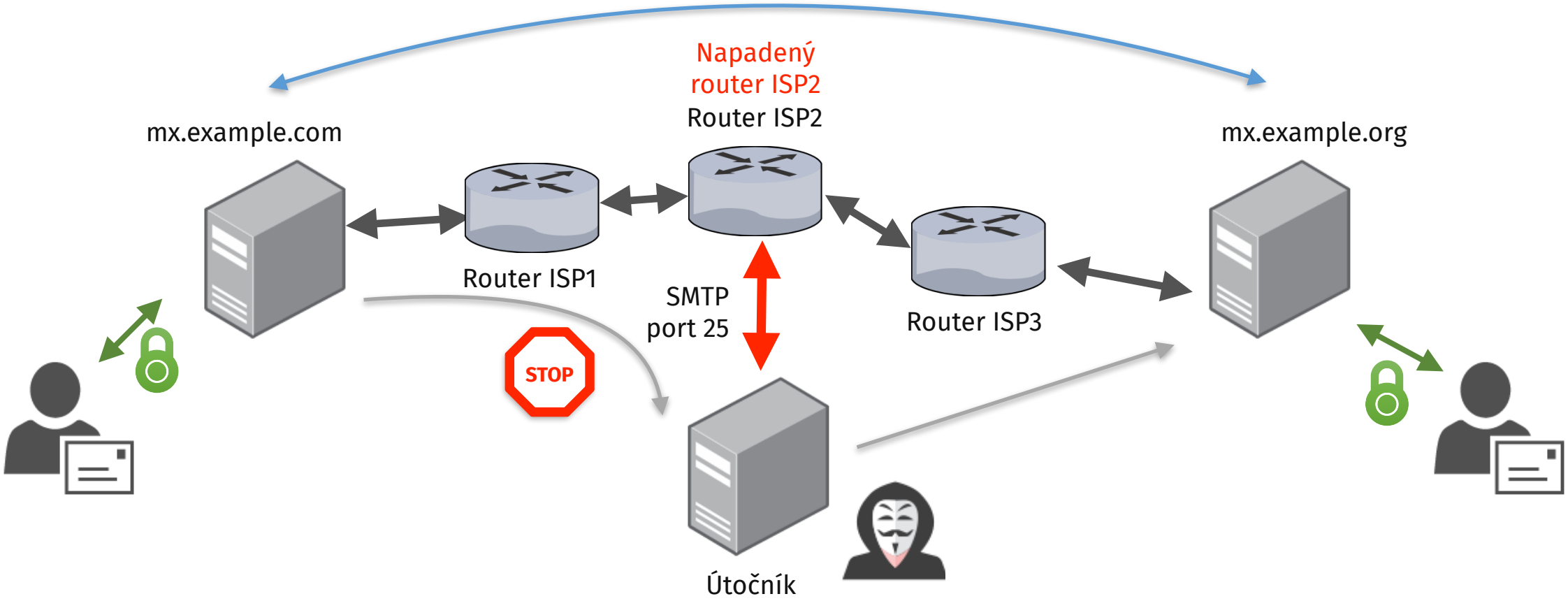
- Vznikl později po DANE, nevyžaduje DNSSEC, iniciativa Google a Microsoftu
- Spočívá v umístění TXT záznamu do DNS a následně souboru na HTTPS serveru
- Sice nevyžaduje DNSSEC, ale bez něj je možné tuto technologii obejít

```
_mta-sts.example.com. 262 IN  TXT "v=STSv1; id=20171114T070707;"
```

```
# https://mta-sts.example.com/.well-known/mta-sts.txt
version: STSv1
mode: enforce
mx: mx.example.com
max_age: 86400
```

Zabezpečení e-mailové komunikace

Přenos informace o certifikátu přes bezpečenou komunikaci:
DANE (DNSSEC)



Naše řešení z roku 2021

Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky
IČO: 05800226
ID datové schránky: zzfnkp3

Spisová značka:
350 - 1117/2021
Číslo jednací:
8477/2021-NÚKIB-E/350

Brno, 11. října 2021

Vyřizuje:
Štěpán Daněk

VEŘEJNÁ VYHLÁŠKA

OPATŘENÍ OBECNÉ POVAHY

Národní úřad pro kybernetickou a informační bezpečnost se sídlem Brno, Mučednická 1125/31, PSČ 616 00 (dále jen „Úřad") jako příslušný ústřední správní úřad podle § 22 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti"),

stanovuje

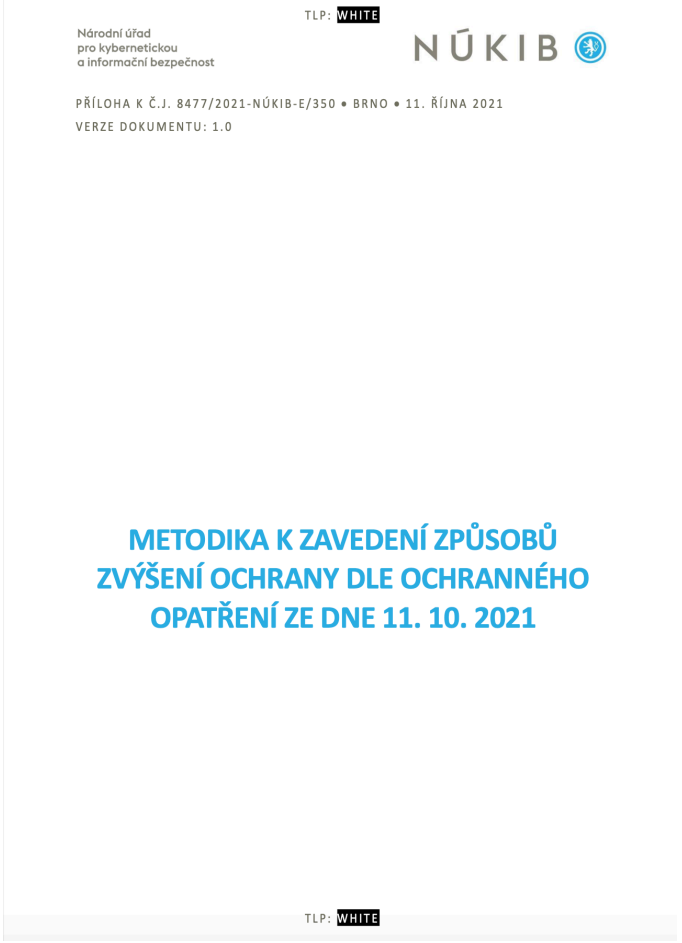
na základě § 14 zákona o kybernetické bezpečnosti a postupem podle § 15 zákona o kybernetické bezpečnosti a § 171, § 173 a § 174 zákona č. 500/2004 Sb., správního řádu, ve znění pozdějších předpisů, **jako ochranné opatření tyto způsoby zvýšení ochrany informačních systémů, služeb a sítí elektronických komunikací:**

1. **Orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti, jejichž elektronická pošta je součástí informačního nebo komunikačního systému, na který se vztahují požadavky zákona o kybernetické bezpečnosti, zajistí, aby při přijímání a odesílání elektronické pošty protokolem SMTP mimo vnitřní síť byly splněny následující požadavky:**

   1.1. Všechny SMTP servery uvedené v MX záznamech, přes které je přijímána elektronická pošta, a hraniční SMTP servery, přes které je pošta odesílána, podporují zabezpečené spojení dle standardu STARTTLS (IETF RFC 3207).

   1.2. V rámci zabezpečeného spojení všechny servery, přes které je přijímána nebo odesílána elektronická pošta:

15 stran



TLP: WHITE

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

PŘÍLOHA K Č.J. 8477/2021-NÚKIB-E/350 • BRNO • 11. ŘÍJNA 2021

VERZE DOKUMENTU: 1.0

METODIKA K ZAVEDENÍ ZPŮSOBŮ ZVÝŠENÍ OCHRANY DLE OCHRANNÉHO OPATŘENÍ ZE DNE 11. 10. 2021

TLP: WHITE

22 stran

TLP: WHITE

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

PŘÍLOHA K Č.J. 8477/2021-NÚKIB-E/350 • BRNO • 11. ŘÍJNA 2021

VERZE DOKUMENTU: 1.0

OCHRANNÉ OPATŘENÍ K ZABEZPEČENÍ E-MAILŮ ZE DNE 11. 10. 2021

Často kladené otázky

7 stran

TLP:CLEAR

Co ochranné opatření vyžaduje

- STARTTLS
- Podporovat pouze algoritmy schválené NÚKIB (TLSv1.2 nebo TLSv1.3, TLSv1.0 nebo TLSv1.1 pouze v nutných případech)
- Certifikát vydaný globálně uznávanou certifikační autoritou
- SPF
- DKIM
- DMARC
- DNSSEC (veřejné instituce musí mít již o roku 2015!)
- DANE
- IMAPS, POP3S, SMTPS, HTTPS nebo TLS only pro komunikaci s klientem
- Strict Transport Security pro webové rozhraní

Proč ne MTA-STS

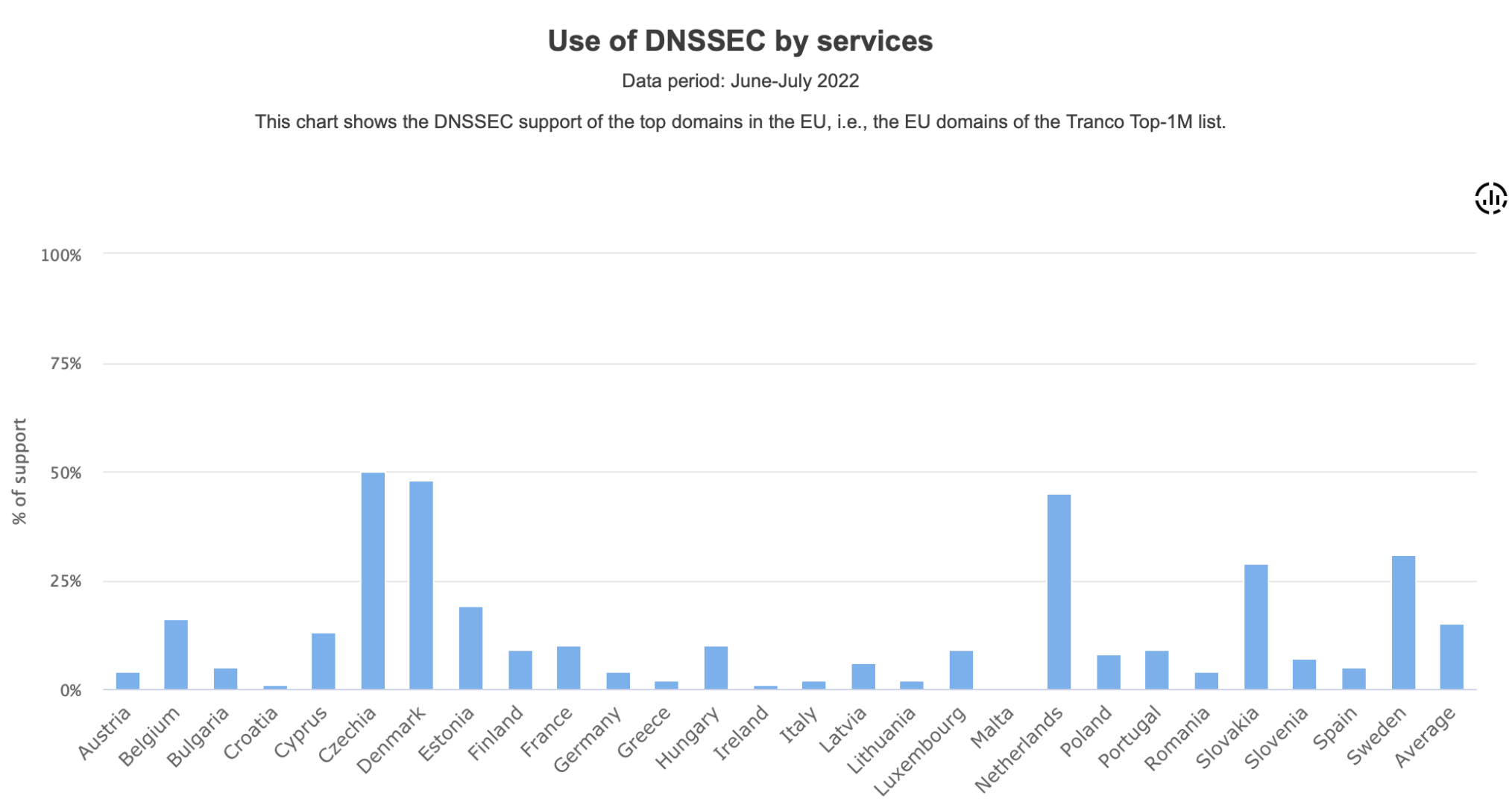
- Komplikované: nutnost měnit DNS záznam a přidat soubor na web
- Náchylné na chybovost
  - vypršení TLS certifikátu na webovém serveru
  - provoz HTTPS serveru
- Poštovní server musí mít prostup na HTTPS do Internetu
  - Potenciální bezpečnostní slabina
- I když nevyžaduje DNSSEC, bez něj je možné zabezpečení obejít
- Minimální podpora v open-source světě
  - Postfix podporuje DANE přímo, MTA-STS pouze pomocí aplikace třetí strany
- MTA-STS vyžaduje validní certifikát SMTP serveru podepsaný uznávanou CA

Proč ne MTA-STS

RFC 8461: SMTP MTA Strict Transport Security (MTA-STS)

The primary motivation of MTA-STS is to provide a mechanism for domains to ensure transport security even when **deploying DNSSEC is undesirable or impractical.**

Proč ne MTA-STS



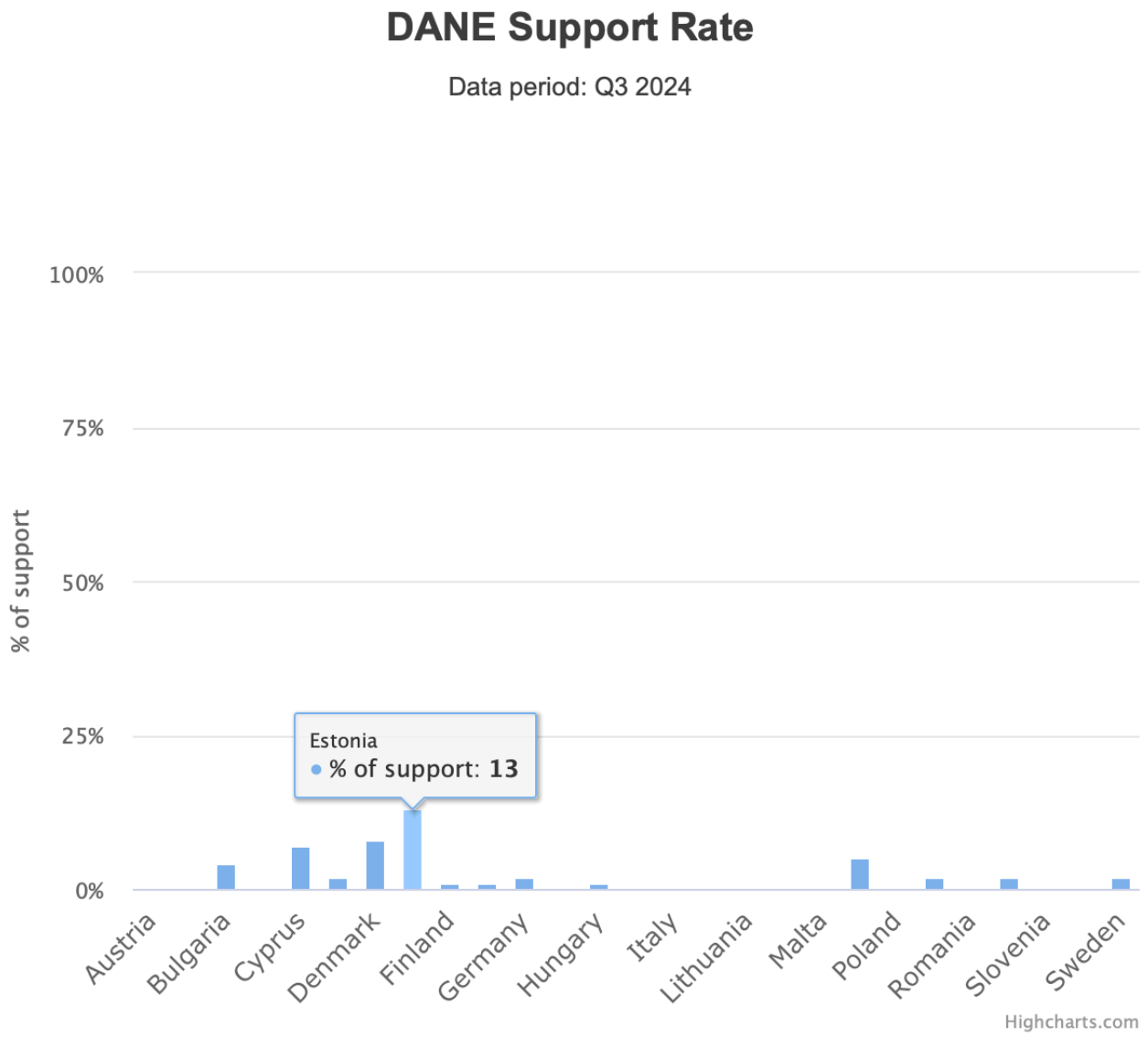
Zdroj: https://ec.europa.eu/internet-standards/dns.html

TLP:CLEAR

Jak jsme na tom po čtyřech letech

TLP:CLEAR

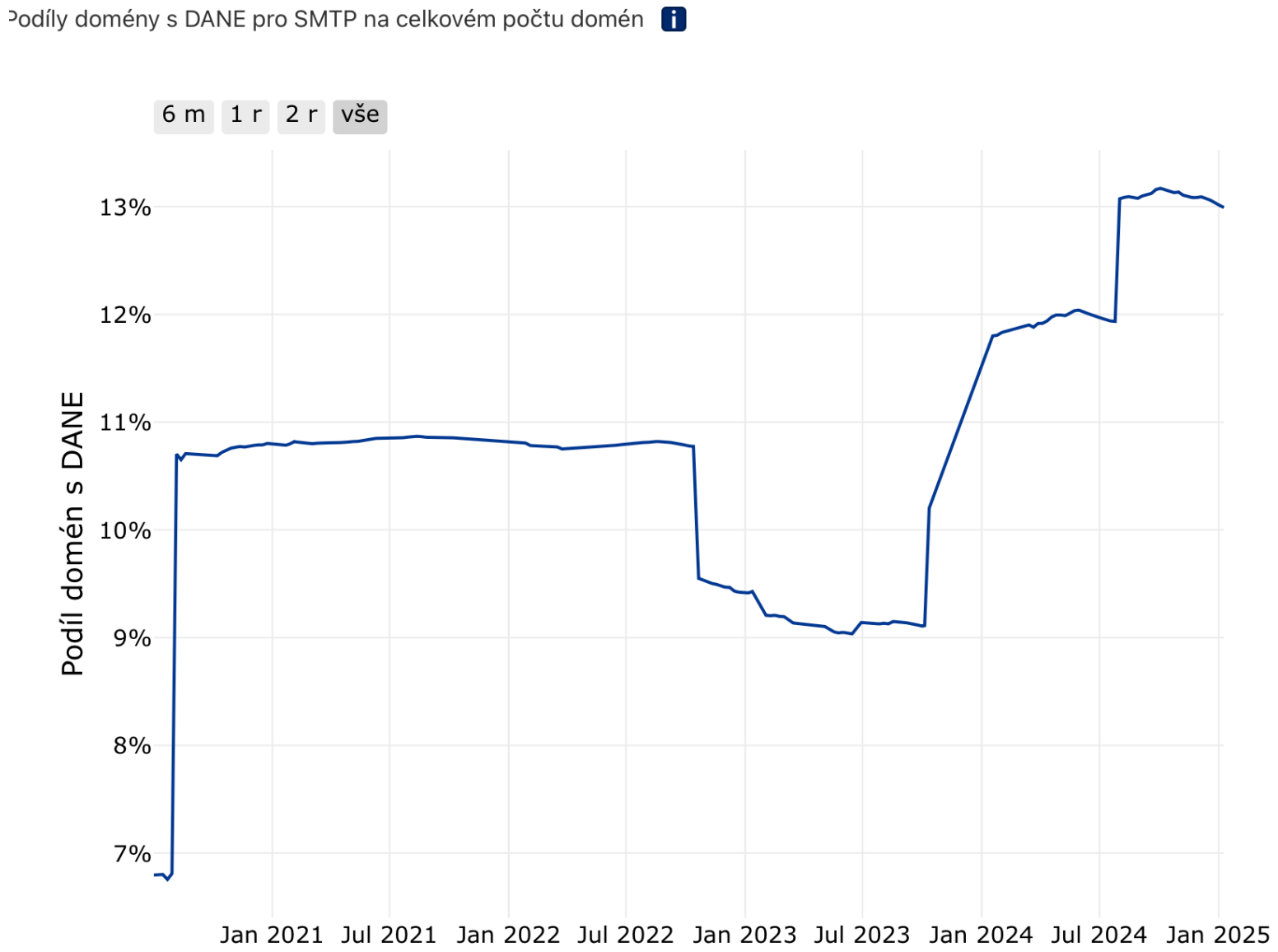
Jak jsme na tom po 4 letech



Zdroj: https://ec.europa.eu/internet-standards/email.html

TLP:CLEAR

Jak jsme na tom po 4 letech



Zdroj: https://stats.nic.cz/dashboard/cs/DNSSEC.html

TLP:CLEAR

Jak jsme na tom po 4 letech

ISP	DNSSEC	DANE
T-Mobile	❌	❌
Vodafone	❌	❌
O2	✅	✅
nej.cz	✅	❌
CETIN	✅	✅
Poda	❌	❌

Bankovní sektor	DNSSEC	DANE
Česká spořitelna	❌	❌
ČSOB	✅	✅
Komerční banka	✅	✅
Moneta	❌	❌
Raiffeisenbank	✅	❌
Unicredit	❌	❌

Co se změní s novým zákonem o kybernetické bezpečnosti (NIS2)?

TLP:CLEAR

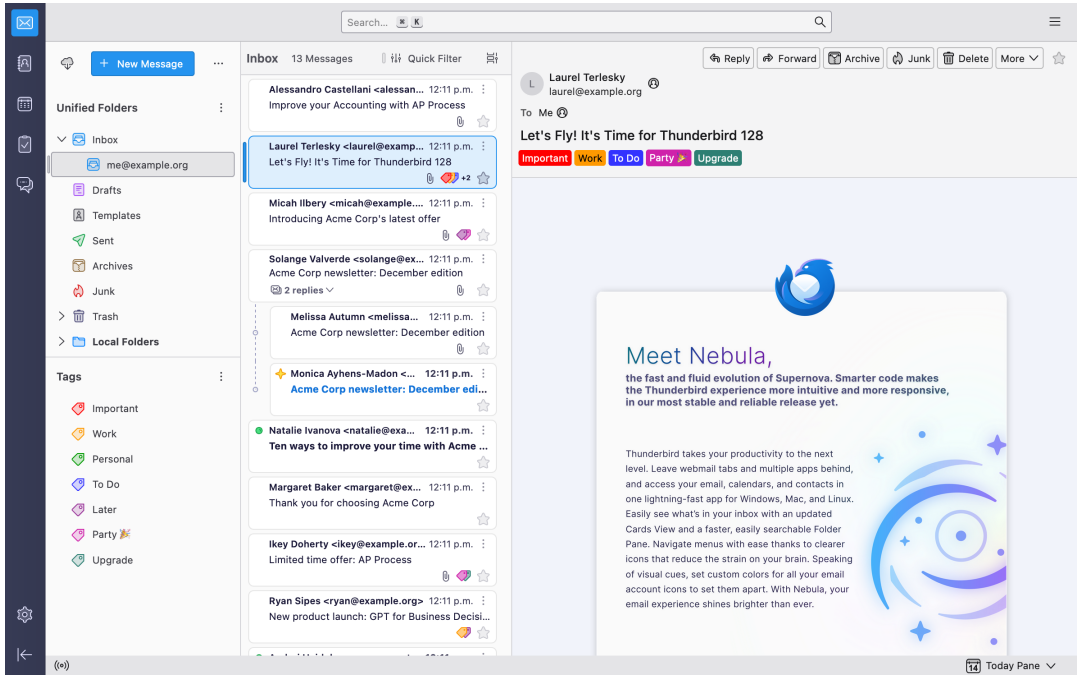
Co se změní s nZKB (NIS2)?

- Zvýšení počtu organizací, které budou muset kybernetickou bezpečnost řešit
- Zvětšení rozsahu regulace u již regulovaných organizací
- **Bezpečnost e-mailové komunikace přímo vyžadována vyhláškami**

- E-mailové systémy jsou dle současného zákona regulovány primárně ve veřejném sektoru (Významný informační systém)
- Dá se předpokládat, že e-mailové systémy budou s nZKB mnohem více regulovány i v soukromém sektoru

Jaké pravidla je nutné dodržovat?

- Připravované vyhlášky ani pro nižší, ani pro vyšší režim nenastavují konkrétní pravidla/technologie pro zabezpečení e-mailové komunikace
  - Vyhláška je obecná – stejnou vyhláškou se řídí např. kybernetická bezpečnost jaderné elektrárny, tak cloudového e-mailového systému



TLP:CLEAR

Jaké pravidla bude nutné dodržovat?

Návrh vyhlášky pro vyšší režim:

§ 25

Aplikační bezpečnost

(1) Povinná osoba pro zajištění bezpečnosti regulované služby užívá technická aktiva, která jsou výrobcem, dodavatelem nebo jinou osobou podporována a zajistí bezodkladné aplikování schválených bezpečnostních aktualizací vydaných pro tato aktiva.

(2) Povinná osoba do doby plnění odstavce 1 zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv a eviduje technická aktiva

a) která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována a

b) na která není možné aplikovat poslední schválenou bezpečnostní aktualizaci.

(3) Povinná osoba v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací, transakcí a přenášených identifikátorů relací před

a) neoprávněnou činností a

b) popřením provedených činností.

(4) Povinná osoba provádí pravidelné skenování zranitelnosti technických aktiv regulované služby

a) z interní a externí komunikační sítě a

b) alespoň jednou ročně.

TLP:CLEAR

Jaké pravidla bude nutné dodržovat?

Návrh vyhlášky pro vyšší režim:

§ 26

Kryptografické algoritmy

(1) Povinná osoba rámci zajištění bezpečnosti technických aktiv a jejich komunikace
a) používá pouze aktuálně odolné kryptografické algoritmy,
b) prosazuje bezpečné nakládání s kryptografickými algoritmy a
c) zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Úřadem, zveřejněné na jeho internetových stránkách.

(2) Povinná osoba zajišťuje bezpečnou
a) hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace, a
b) nouzovou komunikaci v rámci organizace.

(3) Povinná osoba v případě využívání kryptografických klíčů a certifikátů pro ochranu technických aktiv a komunikační sítě používá
a) pouze aktuálně odolné kryptografických klíče a certifikáty a
b) nástroj pro správu kryptografických klíčů a certifikátů, který
1. zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a řádnou likvidaci kryptografických klíčů,
2. umožní kontrolu a audit a
3. zajistí důvěrnost a integritu kryptografických klíčů.

TLP:CLEAR

Jaké pravidla bude nutné dodržovat?

Návrh vyhlášky pro nižší režim:

§ 14

Kryptografické algoritmy

(1) Povinná osoba v rámci zajištění bezpečnostní technických aktiv a jejich komunikace

a) používá aktuálně odolné kryptografické algoritmy,

b) prosazuje bezpečné nakládání s kryptografickými algoritmy a

c) zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Úřadem, zveřejněné na jeho internetových stránkách.

(2) Povinná osoba zajišťuje bezpečnou

a) hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace, a

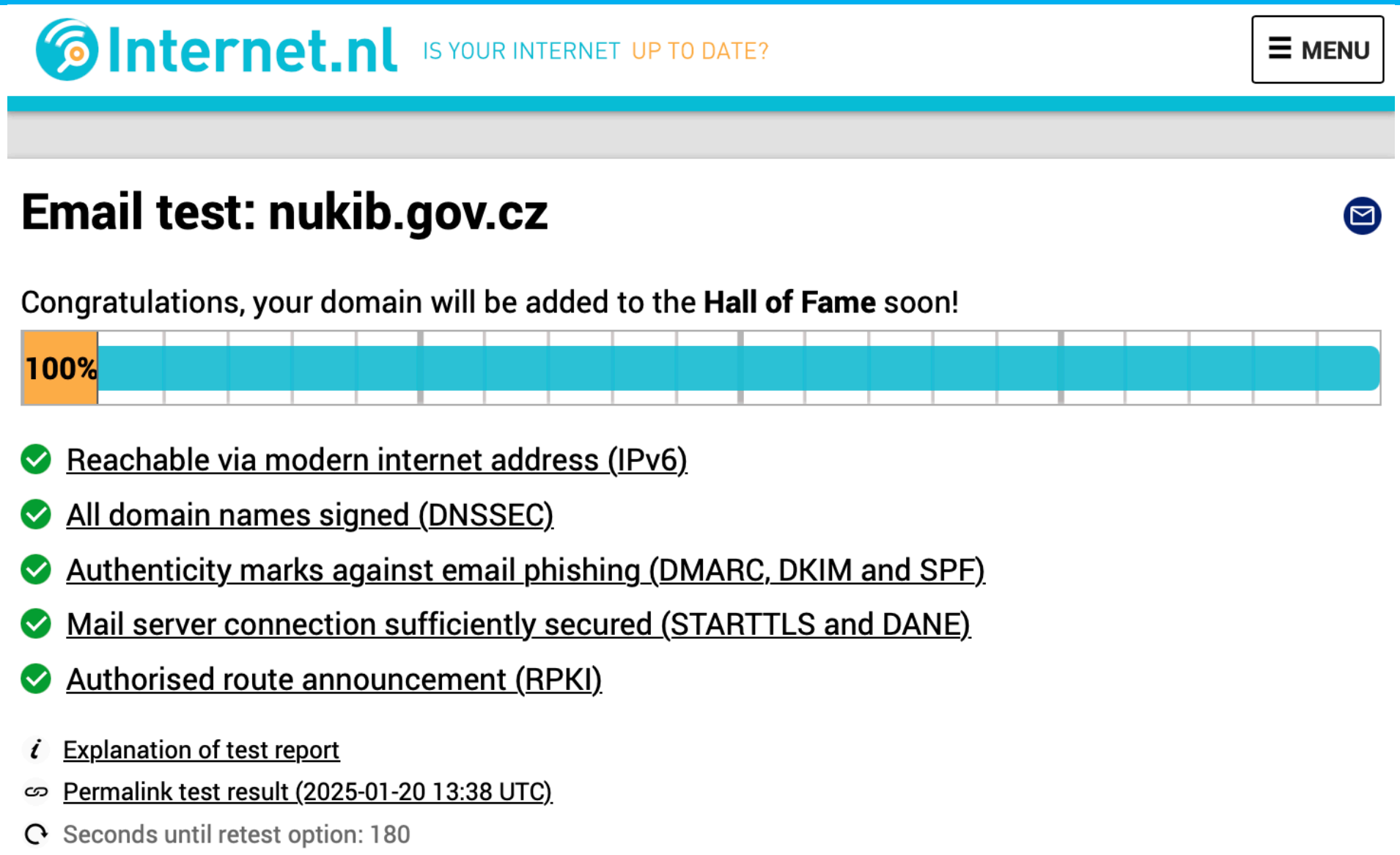
b) nouzovou komunikaci v rámci organizace.

TLP:CLEAR

A co ochranné opatření?

- I s novým zákonem zůstane dále v platnosti
- **Ale týká se pouze již regulovaných organizací**
  - Zjednodušeně: Pokud se na vás toto ochranné opatření nevztahovalo dosud, nebude se na vás vztahovat ani s novým zákonem
  - Pokud by mělo platit i pro nově regulované organizace, muselo by se vydat znovu dle nZKB (reaktivní protiopatření) – nelze nyní předjímat, zda se tak stane – pokud se tak stane, budete informováni přes Portál NÚKIB
- **Přesto poskytuje vodítko, jak si NÚKIB představuje bezpečný e-mailový systém**

Jak jste na tom vy?



TLP:CLEAR

Co si zapamatovat?

- Bezpečnost e-mailová komunikace je důležitá
- nZKB nestanovuje konkrétní technologie
- Konkrétní technologie stanovuje ochranné opatření pro organizace pod současným ZKB
- Doporučujeme zavádět technologie dle OO

Otázky? Komentáře?